IN THE CLAIMS

Please cancel claims 1-5 and substitute the following new claims 6-10.

What is claimed is:

1. (cancelled) ~~A wide area network using the internet as a backbone, comprising:~~

~~a first dedicated line coupled to a first participating ISX/ISP provider of internet access;~~

~~a source router having a channel service unit having an output coupled to said first dedicated line;~~

~~a source firewall circuit having a first port for coupling directly or through a local area network to a first device for which communication over said wide area network (hereafter WAN) is desired, and having a WAN interface coupled to said source router directly or through a local area network, said source firewall functioning to encrypt the payloads of downstream WAN packets being transmitted via the WAN interface to said source router using any encryption method having a user definable key or keys, and for decrypting the payloads of any incoming upstream WAN packets arriving from said source router via said WAN interface using the same encryption method and user definable key or keys that were used to encrypt the outgoing WAN packets;~~

~~one or more routers of other participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers functioning to implement a predetermined private tunnel data path coupling a router of said first ISX/ISP to a router of said endpoint participating ISX/ISP provider through said routers of said participating ISX/ISP providers;~~

~~a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated line to said router of said endpoint ISX/ISP provider;~~

~~a destination firewall circuit having a WAN interface coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to a device for which communication across said wide area network is desired, said firewall functioning to encrypt the payloads of upstream WAN packets being transmitted through said WAN interface to said destination router for transmission to said source router via said private tunnel using the same encryption method used by said source firewall and the same user definable key or keys used by said source firewall circuit, and for decrypting any incoming packets from said source router arriving from said endpoint~~

~~participating ISX/ISP provider using the same encryption protocol used by said source firewall and the same user definable key or keys used by said source firewall circuit and transmitting the decrypted packets to said second device.~~

2. (cancelled) ~~A process for launching downstream AlterWAN packets addressed to an AlterWAN destination into a private tunnel coupling two AlterWAN destinations using the internet as a backbone and for launching non AlterWAN packets into a normal internet traffic routing data path, comprising the steps:~~

~~receiving at a source firewall an incoming downstream wide area network packet from a workstation or other device at a first customer location said incoming downstream wide area network packet being either addressed to an AlterWAN destination or not an AlterWAN packet;~~

~~at said source firewall, using the destination address in said incoming downstream wide area network packet to determine if said packet is addressed to an AlterWAN destination coupled to said source firewall by a private tunnel using the internet as a backbone (hereafter referred to as an AlterWAN packet) or is addressed to some non AlterWAN website or location on the internet (hereafter referred to as a non AlterWAN packet);~~

~~if said packet is an AlterWAN packet, encrypting at said source firewall the payload portion thereof and forwarding the encrypted AlterWAN packet to a source router;~~

~~if said packet is a non AlterWAN packet, at said source firewall, forwarding said non AlterWAN packet to said source router without encrypting the payload portion thereof;~~

~~at said source router, converting both said AlterWAN packets and said non-AlterWAN packets into signals suitable for transmission on a dedicated telephone line or other transmission medium coupling said source router to a specially selected first ISX/ISP provider and transmitting said signals to said specially selected ISX/ISP provider, said specially selected ISX/ISP provider being selected either because their routing tables are such that AlterWAN packets will naturally be routed along high bandwidth, low hop count data paths to the next ISX/ISP provider in said virtual private network or because the routing tables of the router of said first ISX/ISP provider have been altered to insure that AlterWAN packets get routed along high bandwidth, low hop count data paths to the next ISX/ISP provider along said private tunnel.~~

3. (Cancelled) ~~An apparatus comprising:~~

~~a dedicated data path for coupling to a specially selected first participating ISX/ISP provider of internet access;~~

~~a firewall circuit having a first port for coupling directly or through a local area network to one or more devices for which communication over a wide area network using the internet as a backbone is desired, and having a second port, said firewall functioning to to use the destination addresses in the headers of each packet received from said one or more devices to distinguish between AlterWAN packets which are packets addressed to destination devices coupled to said firewall circuit via a private tunnel through the internet, and conventional packets which are packets not addressed to destination devices coupled to said firewall circuit via a private tunnel through the internet, said firewall circuit functioning to encrypt the payloads of outgoing AlterWAN packets using one or more predetermined keys and an encryption algorithem, and sending said encrypted AlterWAN packets to said source router via said second port, and functioning to forward any conventional packets to said source router, and functioning to decrypt any incoming AlterWAN packets arriving from said source router using the the same encryption algorithms and one or more predetermined keys which were used to encrypt the packets at the location from which they were sent;~~

~~a source router having an input coupled to said second port of said firewall circuit either directly or by a local area network connection, and having a channel service unit having an output coupled to said dedicated data path, said channel service unit functioning to convert digital data packets received from said firewall circuit into signals suitable for transmission over whatever type of transmission medium is selected for said dedicated data path, and for converting signals received from said dedicated data path into data packets, said source router for transmitting both AlterWAN and non AlterWAN packets over said dedicated data path to said specially selected first participating ISX/ISP provider where AlterWAN packets will be routed via said private tunnel and specially seleted ISX/ISP providers to their destination and non AlterWAN packets will be routed along paths on the internet other than said private tunnel.~~

4. (Cancelled) ~~A method of designing and implementing a wide area network using the internet as a backbone, comprising the steps:~~

~~1) selecting source and destination sites that have devices that need to be connected by a wide area network;~~

~~2) examining the ISX/ISP internet service providers that exist between said source and destination sites and selecting two or more of such ISX/ISP providers through which data passing between said source and destination sites will be routed, said selection being based upon how many hops the routers at those sites will cause packets travelling between said source and destination sites to take and whether the average available bandwidth of the data paths along which the packets travelling between said source and destination sites will travel is substantially greater than the worst case bandwidth consumption of traffic between said source and destination sites;~~

~~3) coupling a source firewall to the devices at said source site and configuring said firewall to examine the destination addresses of packets received from said devices at said source site and encapsulate each packet addressed to any device at said destination site in an internet protocol packet, hereafter referred to as an AlterWAN packet, said AlterWAN packet having as its destination address the address of an untrusted port of a destination firewall at said destination site and having the original IP packet as its payload, said source firewall being configured to encrypt the payload portions of all said AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but not to encapsulate or encrypt the payload portions of any packets received from said devices at said source site which are not addressed to any device at said destination site, and configuring said source firewall to recognize any incoming AlterWAN packets which have as their destination addresses the IP address of the untrusted side of said source firewall and to strip off the AlterWAN packet headers and decrypt the payload portion of each said AlterWAN packet to recover the original IP packet transmitted from said destination site using the same encryption algorithm and the same encryption key or keys used to encrypt the payload portions of said AlterWAN packets at said destination site and for outputting said recovered the original IP packet to said devices at said source site, said source firewall having an untrusted port;~~

~~4) coupling a source router to receive said encrypted and non-encrypted packets from said untrusted port of said source firewall and to convert them in a channel service unit to signals suitable for transmission over a first dedicated local loop connection;~~

~~5) contracting to establish said first dedicated local loop connection between the output of said source router at which said signals appear and a first participating ISX/ISP provider in the group of ISX/ISP providers selected in step 2;~~

~~6) providing a destination router at said destination site having a channel service unit which functions to receive from a second dedicated local loop connection downstream signals encoding both encrypted AlterWAN packet and conventional IP packets and converting said signals back into the original digital packet form and outputting the recovered downstream packets at a firewall port, and said destination router configured to receive upstream AlterWAN and conventional packets and convert them into signals suitable for transmission on said second dedicated data path coupling said destination router to an endpoint participating ISX/ISP provider in the group of ISX/ISP providers selected in step 2 and transmitting said signals on said second dedicated local loop connection;~~

~~7) contracting to provide a second dedicated local loop connection connecting the input of said destination router to said endpoint participating ISX/ISP provider, said second dedicated local loop connection having sufficiently high bandwidth to handle the worst case traffic volume;~~

~~8) providing a destination firewall having an untrusted port having an IP address coupled to said firewall port of said destination router to receive said recovered digital packets, and configuring said destination firewall to recognize as AlterWAN packets incoming recovered packets having as their destination address the IP address of said destination firewall untrusted input port and to strip off the AlterWAN packet header and decrypt the payload portion of said AlterWAN packet using the same encryption algorithm and encryption key or keys that were used to encrypt the packet at said source firewall, and configuring said destination firewall to output the decrypted packets at an output coupled to devices at said destination site, and configuring said destination firewall to examine the destination addresses of upstream IP packets received from said devices at said destination site and encapsulate each upstream IP packet addressed to any device at said source site in another IP packet, hereafter referred to as an AlterWAN packet, said AlterWAN packet having as its destination address the IP address of an untrusted port of said source firewall at said source site and having the original IP packet as its payload, said destination firewall being configured to encrypt the payload portions of all said AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but not to encapsulate or encrypt the payload portions of any IP~~

~~packets received from said devices at said destination site which are not addressed to any device at said source site (hereafter referred to as conventional packets), and said destination firewall configured to transmit said encrypted AlterWAN packets and said conventional packets to said destination router via said untrusted port.~~

5. (Cancelled) ~~A wide area network using the internet as a backbone, comprising:~~

~~a first dedicated line coupled to a first participating ISX/ISP provider of internet access;~~

~~a source router having a channel service unit having an output coupled to said first dedicated line;~~

~~a source firewall circuit having a first port for coupling directly or through a local area network to a first device for which communication over said wide area network (hereafter WAN) is desired, and having a WAN interface coupled to said source router directly or through a local area network, said source firewall functioning to encrypt the payloads of downstream WAN packets being transmitted via the WAN interface to said source router using a first encryption method having a first set of user definable keys which may be only one key, and for decrypting the payloads of any incoming upstream WAN packets arriving from said first participating ISX/ISP using a second encryption method which is different than said first encryption method and a second set of user definable keys which are different than the first set of user definable keys were used to encrypt the downstream WAN packets;~~

~~one or more routers of other participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers functioning to implement a predetermined private tunnel data path coupling a router of said first ISX/ISP to a router of said endpoint participating ISX/ISP provider through said routers of said participating ISX/ISP providers;~~

~~a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated line to said router of said endpoint ISX/ISP provider;~~

~~a destination firewall circuit having a WAN interface coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to a device for which communication across said wide area network is desired, said destination firewall functioning to encrypt the payloads of upstream WAN packets being transmitted through said WAN interface to said destination router for transmission to said source~~

~~router via said private tunnel using the same encryption method and user definable key or keys used by said source firewall to decrypt upstream WAN packets, and for decrypting any incoming downstream WAN packets from said source router arriving from said destination router via the router of said endpoint participating ISX/ISP provider using the same encryption method and encryption key or keys used by said source firewall to encrypt downstream WAN packets and transmitting the decrypted packets to said second device.~~

6. (Currently Amended) A private, secure wide area network using the internet as a backbone between a source site and a destination site ~~using the internet as a backbone~~, comprising:

a first dedicated ~~local loop connection providing a~~ signal path to a router of a source ISX/ISP provider of internet access;

a source router located at a source site and having a channel service unit having an output coupled to said first dedicated signal path ~~local loop connection~~ and having a routing table which has been configured to recognize AlterWAN packets and always route them over said first dedicated signal path to said source ISX/ISP provider, said AlterWAN packets being packets having as their destination address one of one or more predetermined Internet Protocol addresses assigned to an AlterWAN private tunnel, and AlterWAN private tunnel being a data path through the internet which uses only high bandwidth, low latency data paths between predetermined ISX/ISP provider sites which have been pre-tested to ensure that adequate bandwidth and low latency exists for AlterWAN packets and that AlterWAN packets are always routed at said predetermined ISX/ISP provider site into said AlterWAN private tunnel;

a source firewall circuit located at a source site and having a first port for coupling directly or through a local area network to one or more computers or other devices at said source site for which communication over said private, secure wide area network (hereafter WAN) is desired, and having a WAN interface coupled to said source router directly or through a local area network, said source firewall functioning to encapsulate any Internet Protocol packets hereafter IP packets transmitted from said first computer or other device which have a destination Internet Protocol address (hereafter IP address) which is one of a set of "predetermined IP addresses", said "predetermined IP addresses" being IP addresses of computers or other devices at a destination site which are assigned to said private tunnel, said encapsulation being performed on ~~into~~ the payload sections of IP packets having as their destination address one of said “predetermined IP addresses”, hereafter referred to as AlterWAN packets ~~the IP address of a firewall at said destination site~~ and for encrypting said payload sections of said AlterWAN packets using any encryption method known to a destination firewall at a destination site ~~having a key~~, and transmitting said AlterWAN packets to said source router, ~~where IP packets having as their destination address the IP address of a computer or other device at either said source site or said destination site and having an encrypted IP packet transmitted from a computer or other device at said source site or said destination site as a payload being defined and hereafter referred to as AlterWAN packets~~, but said source firewall for not encapsulating ~~into AlterWAN packets~~ any IP packets transmitted by said first computer or other device which do not have as their destination address one of said “predetermined IP addresses” ~~an IP address which is one of said IP addresses of computers or other devices at said destination site~~, and for receiving incoming IP packets from various sources including computers and devices at said destination site via said source router and for recognizing AlterWAN packets among these IP packets on the basis that an AlterWAN packet has one of said “predetermined IP addresses” as its destination address, and decrypting the payloads of said AlterWAN packets ~~using the same encryption method and key or keys that were used to encrypt the AlterWAN packets~~ to recover said IP packets that were encapsulated in said AlterWAN packets and transmitting at least said recovered IP packets to said one or more computers or devices at said source site to which said recovered IP packets are addressed;

one or more internet data paths coupled to routers of said predetermined ~~other participating~~ ISX/ISP providers of internet services, said routers having their routing tables configured to recognize said AlterWAN packets by their destination addresses and to cause said routers to route AlterWAN packets into said AlterWAN private tunnel data path, each ~~besides said source ISX/ISP provider including a router at an endpoint participating ISX/ISP provider, said routers of said source and endpoint ISX/ISP providers and said other participating ISX/ISP providers functioning to implement a predetermined private tunnel data path for said AlterWAN packets coupling a router of said source ISX/ISP provider to a router of said endpoint participating ISX/ISP provider through said routers of said other participating ISX/ISP providers, said source and endpoint ISX/ISP providers and~~ said predetermined ~~other~~ ISX/ISP ~~providers being providers~~ provider being a provider of internet services who has ~~have~~ contracted to provide routing of AlterWAN packets into said AlterWAN private tunnel data path, said AlterWAN private tunnel data path being at least one of said internet data paths which has ~~and who have~~ been pretested ~~pretested~~ to verify that said data path does ~~they do~~ in fact provides a low hop count data path having ~~portion of a data path between a said source site and a said destination site for said AlterWAN packets with~~ an average available bandwidth along each ~~said~~ portion of said data path travelled by said AlterWAN packets which ~~each ISX/ISP provider provides which~~ ~~substantially~~ exceeds the worst case bandwidth consumption of AlterWAN packet traffic between said source site and said destination site;

a destination router including a channel service unit coupled to or part of said destination router and having a trusted side output, said destination router coupled through said channel service unit and a second dedicated data path ~~local loop connection~~ to ~~said~~ a router of a said participating ~~endpoint~~ ISX/ISP provider, said destination router having its routing tables configured to recognize said AlterWAN packets and route them to said trusted side output;

a destination firewall circuit having a WAN interface coupled to said trusted side output of said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to a one or more computers or devices for which communication across said private AlterWAN data path~~,~~ ~~secure wide area network~~ is desired, said destination firewall functioning to encapsulate into the payload sections of AlterWAN packets IP packets transmitted from said one or more computers or devices at said destination site and having as their destination addresses one of said “predetermined IP addresses” which is an IP address of said one or more computers or devices at said source site, and functioning to encrypt the payloads of said AlterWAN packets and transmit said AlterWAN packets to said destination router, but for not encapsulating into AlterWAN packets any IP packets transmitted from said one or more computers or devices at said destination site which do not have as their destination address one of said “predetermined IP addresses” ~~an IP address of said one or more computers or devices at said source site~~, and for receiving IP packets from various sources including said one or more computers or devices at said source site via said destination router, and functioning to recognize AlterWAN packets among said received IP packets and decrypt the payload sections of said AlterWAN packets to recover the original IP packets ~~using the same encryption protocol used by said source firewall to encrypt said payload sections of said AlterWAN packets and the same key or keys used by said source firewall~~ and transmitting at least the decrypted IP packets recovered from AlterWAN packet to said one or more computers or devices at said destination site.

7. (Currently Amended) A process for sending AlterWAN data packets securely between a computer at a source site and a computer at a destination site so as to implement a private Wide Area Network (hereafter AlterWAN) between said source and destination sites of a customer, said AlterWAN using the internet as a backbone but which is private and which only said customer can use ~~while simultaneously launching non AlterWAN packets into a normal internet traffic routing data path~~, comprising the steps:

receiving at a source firewall incoming Internet Protocol packets (hereafter IP packets) from a computer~~s~~ at a source site of a customer, some of said IP packets having as their destination addresses an Internet Protocol address (hereafter IP address) which is one of one or more IP addresses of ~~a computer~~ one or more computers or other computing devices at a destination site of said customer;

at said source firewall, comparing the destination address in each said received IP packet to an IP address of a computer at said destination site of said customer, and if an IP packet has as its destination address the IP address of a computer or other computing device at said destination site (hereafter referred to as an AlterWAN inner packet), concluding said IP packet is an AlterWAN inner packet ~~payload~~ which needs to be transmitted ~~via a virtual private network over the internet~~ to said computer or other computing device at said destination site via a high bandwidth, low latency, low hop count data path using said internet as a backbone and connecting said source site to said destination site and having an average available bandwidth which exceeds the worst case bandwidth consumption of packets traveling between said source site and said destination site (hereafter referred as the AlterWAN data path), but if said destination address of said received IP packet is not an IP address of a computer or other computing device at said destination site, concluding said IP packet is ~~nont~~ an AlterWAN inner ~~payload~~ packet and needs to be routed like ~~as~~ any other IP packet would be routed;

if ~~a~~ said received IP packet is an AlterWAN inner ~~payload~~ packet, encapsulating said AlterWAN inner ~~payload~~ packet into the payload section of a second ~~an~~ IP packet having as its destination address the IP address of an untrusted side of a firewall at said ~~the~~ destination site ~~end~~ of said AlterWAN data path ~~virtual private network~~ (hereafter referred to as composite AlterWAN packet) and encrypting at said source firewall at least ~~the~~ a payload portion of said AlterWAN inner packet using any encryption algorithm which can be decrypted by said firewall at said destination site ~~having a key which same encryption algorithm and key can be used by a firewall at said destination site to recover said AlterWAN payload packet~~, and forwarding said composite AlterWAN packet to a source router;

if ~~a~~ said received IP packet is not an AlterWAN inner ~~payload~~ packet, forwarding said received IP packet ~~which is not an AlterWAN payload packet~~ (hereafter referred to as a non-AlterWAN packet) to said source router without encapsulating said non-AlterWAN packet into ~~an~~ a composite AlterWAN packet;

at said source router, converting both said composite AlterWAN packets and said non-AlterWAN packets into signals suitable for transmission on a dedicated signal path ~~local loop connection~~ coupling said source router to a ~~specially selected~~ predetermined source participating ISX/ISP provider of internet connectivity and routing services, and transmitting said signals to said ~~specially selected~~ predetermined source participating ISX/ISP provider, said predetermined ~~specially selected~~ source participating ISX/ISP provider being selected because said provider has available a high bandwidth, low latency, low hop count data path which is part of said AlterWAN data path and also has agreed to route said chomposite AlterWAN packets into said AlterWAN data path and has routers wich either already contain routing statements which will route said AlterWAN packets into said AlterWAN data path or which have been configured to contain such a routing statement or statements. ~~either because their routing tables are such that AlterWAN packets will naturally be routed along high bandwidth, low hop count data paths to next participating ISX/ISP provider in said virtual private network or because the routing tables of the router of said specially selected source participating ISX/ISP provider have been altered to insure that AlterWAN packets get routed along high bandwidth, low hop count data paths to the next ISX/ISP provider along said virtual private network and wherein said source participating ISX/ISP provider and all other participating ISX/ISP providers whose routers route AlterWAN packets have contracted to provide a data path for said AlterWAN packets with an average available bandwidth which exceeds the worst case bandwidth consumption of AlterWAN packets traveling between said source site and said destination site of said customer.~~

8. (Currently amended) An apparatus comprising:

a dedicated data path for coupling signals to a specially selected first participating ISX/ISP provider of internet access;

a first firewall circuit having a first port for coupling directly or through a local area network to one or more computing devices for which is desired communication over a private wide area network between a customer's source site and destination site using the internet as a backbone ~~is desired~~, and having a second port, said firewall functioning to use the destination addresses in the headers of each packet received from said one or more computing devices at said source site to distinguish between conventional packets and AlterWAN payload packets, where AlterWAN payload packets are packets having as their destination addresses an address of a computing device ~~addressed to devices~~ at said destination site or said source site, and wherein a computing device ~~computer~~ at said destination site is coupled to a computer ~~computing device~~ at said source site via a second firewall circuit and an AlterWAN data path comprising of a virtual private network tunnel implemented along a high bandwidth, low latency, low hop count data paths through a public wide area network such as the internet terminating at said source site at an untrusted side of said first firewall circuit and terminating at said destination site at an untrusted side of said second firewall circuit, and wherein conventional packets are packets which are not addressed to any computing device ~~devices~~ at said destination site, said first firewall circuit functioning to encapsulate said AlterWAN payload packets in the payload section of AlterWAN packets which have as their destination address the address of said untrusted side of ~~are addressed to~~ said second firewall circuit at said destination end of said virtual private network tunnel, ~~and~~ said first firewall circuit further functioning to encrypt the payloads (AlterWAN payload packet) of AlterWAN packets ~~using one or more predetermined keys and an encryption algorithm~~, and distinguishing ~~said first firewall circuit further functioning to distinguish~~ between incoming AlterWAN packets from said destination site and conventional packets by comparing the destination addresses thereof to the address of said untrusted side of said first firewall circuit and concluding that any incoming packets addressed to said first firewall circuit are AlterWAN packet and all packets addressed to one or more computing devices ~~computers~~ at said source site coupled to said first firewall circuit are conventional packets, and further functioning to decrypt the payload sections of any incoming AlterWAN packets ~~using the same encryption algorithm and one or more predetermined keys which were used to encrypt the AlterWAN packets~~ so as to recover the encapsulated AlterWAN payload packet;

a source router having an input coupled to said second port of said first firewall circuit either directly or by a local area network connection, and having a channel service unit having an output coupled to said dedicated data path, said router and channel service unit functioning to receive said AlterWAN packets and said conventional packets from said first firewall circuit and convert said packets into signals suitable for transmission over whatever type of transmission medium is selected for said dedicated data path, and for converting signals received from said dedicated data path into data packets, said source router for transmitting both AlterWAN packets and conventional packets received from said first firewall over said dedicated data path to said specially selected first participating ISX/ISP provider where said AlterWAN packets will be routed ~~via said virtual private network tunnel and specially selected participating ISX/ISP providers~~ via said AlterWAN data path to said second firewall ~~and non-AlterWAN packets will be routed along paths on the internet other than said virtual private network tunnel~~ and wherein said AlterWAN data path has ~~first participating ISX/ISP provider and all said other ISX/ISP providers are providers who have contracted to and do in fact provide data paths for AlterWAN packets which combine to form a low hop count data path with~~ an average available bandwidth which substantially exceeds the worst case bandwidth consumption of AlterWAN packets traveling between said source site and said destination site.

9. (Currently amended) A method of designing and implementing a private wide area network using the internet as a backbone carrying data packets between a source site to a destination site hereafter referred to as an AlterWAN data path), comprising the steps:

1) selecting source and destination sites that have computers or other devices (hereafter referred to simply as computers) that need to be connected by a wide area network;

2) examining available ISX/ISP internet service providers that can route ~~AlterWAN~~ packets between said source and destination sites and selecting two or more of such ISX/ISP providers as participating ISX/ISP providers including at least a source ISX/ISP provider and a destination ISX/ISP provider through which ~~AlterWAN~~ packet data passing between said source and destination sites will be routed, said selection of said participating ISX/ISP providers being made upon the availability to said participating ISX/ISP providers of one or more high bandwidth, low latency data paths which will form part of said AlterWAN data path, said participating ISX/ISP providers agreeing to route packets travelling between said source site and said destination site (hereafter AlterWAN packets) into said AlterWAN data path and agreeing to allow route statements to be added to their routers to cause AlterWAN packets to always be routed into said AlterWAN data path, ~~so as to minimize the number of hops on the internet the routers at participating ISX/ISP providers will cause AlterWAN packets to take while traveling between said source and destination sites and so as to~~ said participating ISX/ISP providers also agreeing to manage their portions of said AlterWAN data path so as to guarantee that the average available bandwidth of their portion of said AlterWAN data path ~~the data paths along which said AlterWAN packets traveling between computers at~~

~~said source and destination sites will travel~~ is substantially greater than the worst case bandwidth consumption of AlterWAN packet traffic between said source and destination sites;

3) adding route statements to routers of said participating ISX/ISP providers which will to cause AlterWAN packets to always be routed into said AlterWAN data path and pretesting said ~~the~~ ISX/ISP providers selected in step 2 by testing to verify the data path that ~~an~~ AlterWAN packets travel will be a portion of said AlterWAN data path and that performance is adequate; ~~take through the internet to verify that what the participating ISX/ISP providers promised to deliver will actually be delivered;~~

~~4) contracting with said participating ISX/ISP providers to provide routing of AlterWAN packets so as to minimize the number of hops on the internet said AlterWAN packets need to take in traveling between said source and destination sites and so as to guarantee that the average available bandwidth along data paths AlterWAN packets must traverse to travel between said source and destination sites is substantially greater than the worst case bandwidth consumption of traffic between source and destination sites, and, if necessary, configuring data in routing tables of said participating ISX/ISP providers so as to minimize said number of hops and guarantee said bandwidth contracted for when routing AlterWAN packets;~~

4 ~~5~~) contracting to establish and establishing a first dedicated signal path ~~local loop connection~~ between the output of a source router at which said signals appear and said source ISX/ISP provider in said ~~the~~ group of participating ISX/ISP providers selected in step 2, said first dedicated signal path ~~local loop connection~~ having sufficiently high bandwidth to handle the worst case traffic volume in AlterWAN packets ~~traveling between said source and destination sites~~;

5 ~~6~~) contracting to provide a second dedicated signal path ~~local loop connection~~ connecting the input of a destination router to said destination ISX/ISP provider, said second dedicated local loop connection having sufficiently high bandwidth to handle the worst case traffic volume in AlterWAN packets ~~traveling between said source and destination sites~~;

6 ~~7~~) coupling an untrusted port of a source firewall/virtual private network circuit (hereafter referred to as the source firewall) to a source router and coupling a trusted port of said source firewall to ~~said~~ one or more computing device or devices at said source site and configuring said source firewall to examine the destination addresses of a first internet Protocol packet~~s~~ (hereafter IP packet~~s~~) received from one of ~~said~~ one or more computing devices at said source site and encapsulating ~~encapsulate~~ each first IP packet

having as its destination address and address which is a ~~the~~ Internet Protocol address (hereafter IP address) of any computing device at said destination site as a payload portion in a second IP packet, said second IP packet hereafter referred to as an AlterWAN packet, said AlterWAN packet having as its destination address the IP address of an untrusted port of a destination firewall/virtual private network circuit (hereafter referred to as the destination firewall) at said destination site and having an encrypted version of at least the payload section of said first ~~the original~~ IP packet as its payload, said source firewall being configured to recognize non AlterWAN packets and with portions of said AlterWAN packet other than said payload section being referred to herein as an AlterWAN packet header~~, said source firewall also being configured to encrypt the payload portions of all said AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but~~ not to encapsulate or encrypt the payload portions of any non AlterWAN packets received from one or mor of said devices at said source site which do not have as their destination address an ~~the~~ IP address of any device at said destination site ~~(hereafter referred to as non AlterWAN packets)~~, and configuring said source firewall to screen incoming IP packets from said destination firewall so as to recognize any incoming AlterWAN packets which have as their destination addresses the IP address of the untrusted port of said source firewall and to strip off said ~~the~~ AlterWAN packet headers and decrypt a ~~the~~ payload portion of each said incoming AlterWAN packet to recover the original IP packet transmitted from said destination firewall ~~using the same encryption algorithm and the same encryption key or keys used to encrypt the payload portions of said AlterWAN packets when they were transmitted from said destination firewall~~ so as to recover the original IP packet transmitted to said destination firewall by a computer at said destination site, and for outputting said recovered original IP packet to said device or devices at said source site having the IP address which is the destination address of said original IP packet;

7 ~~8)~~ coupling a source router to receive said ~~encrypted~~ AlterWAN packets and ~~non-encrypted~~ non-AlterWAN packets from said ~~untrusted port of said~~ source firewall and to convert said AlterWAN and non-AlterWAN packets in a channel service unit to signals suitable for transmission over said first dedicated signal path ~~local loop connection~~ to said source ISX/ISP provider;

8~~9)~~ providing a destination router at said destination site having a firewall port coupled to an ~~said~~ untrusted port of said destination firewall and having a channel service unit coupled to said destination ISX/ISP provider via said second dedicated signal path ~~local loop connection~~ and configuring said destination router ~~which is configured~~ to receive from said second dedicated signal path ~~local loop connection~~ downstream signals encoding both encrypted AlterWAN packets and conventional non AlterWAN IP packets and convert ~~converting~~ said signals back into the original digital IP packet form, and configuring said destination router to output said recovered downstream IP packets at said firewall port coupled to said untrusted port of said destination firewall, and configuring said destination router ~~configured~~ to receive upstream AlterWAN packets and conventional non AlterWAN packets and convert both types of said packets into signals suitable for transmission on said second dedicated signal path ~~local loop connection~~ coupling said destination router to said participating destination ISX/ISP provider in said ~~the~~ group of participating ISX/ISP providers selected in step 2, and configuring said router to transmit ~~transmitting~~ said signals on said second dedicated signal path ~~local loop connection~~;

9 ~~10~~) providing said ~~a~~ destination firewall having an untrusted port coupled to said firewall port of said destination router so as to receive said recovered digital IP packets, and configuring said destination firewall to recognize as AlterWAN packets incoming recovered IP packets having as their destination address the IP address of said destination firewall untrusted port and further configuring said destination firewall ~~configured~~ to strip off said ~~the~~ AlterWAN packet header of each said AlterWAN packet and, as to each AlterWAN packet, decrypting a ~~the~~ payload portion of ~~each~~ said AlterWAN packet ~~using the same encryption algorithm and encryption key or keys that were used to encrypt the AlterWAN packet at said source firewall~~ so as to recover said first ~~the original~~ IP packet which encapsulated in said ~~each~~ AlterWAN packet, and configuring said destination firewall to output said first IP packet recovered from said AlterWAN packet by said decryption process ~~the decrypted original~~ and output each said first IP packet~~s~~ so recovered at an output coupled to one or more computing ~~a device or~~ devices at said destination site, and configuring said destination firewall to examine the destination addresses of upstream first IP packets received from said one or more computing ~~a device or~~ devices at said destination site and encapsulate each upstream first IP packet addressed to any computer or other computing device at said source site as a ~~the~~ payload portion of ~~in~~ a second ~~another~~ IP packet, hereafter referred to as an upstream AlterWAN packet (an AlterWAN packet traveling from said destination site toward said source site), each said upstream AlterWAN packet having as its destination address the IP address of said untrusted port of said source firewall at said source site and a first ~~having the original~~ IP packet as its payload, and further configuring said said destination firewall ~~being configured~~ to encrypt the payload portions of each ~~all~~ said

upstream AlterWAN packet~~s using a predetermined encryption algorithm and one or more encryption keys~~ but not to encapsulate or encrypt ~~the~~ payload portions of any non AlterWAN IP packets received from said one or more computing ~~device or~~ devices at said destination site, said non AlterWAN IP packets being those IP packets which do not have as their destination addresses an IP address of any device at said source site ~~(hereafter referred to as conventional non AlterWAN packets)~~, and configuring said destination firewall ~~configured~~ to transmit said encrypted upstream AlterWAN packets and said conventional non AlterWAN packets to said destination router via said untrusted port.

10. (Currently amended) A private wide area network connecting a customer source site to a customer destination site and using the internet as a backbone, comprising:

a first dedicated data path coupled to a first participating ISX/ISP provider of internet access;

a source router having a channel service unit having an output coupled to said first dedicated data path and configured with route statements that recognize IP packets addressed to the untrusted side of a destination firewall at said customer destination site (hereafter outgoing AlterWAN packets) and cause said outgoing AlterWAN packets to be routed into an AlterWAN data path, wherein said AlterWAN data path is a high bandwidth, low latency data path from said customer source site to said customer destination site and back having an average available bandwidth that exceeds the worst case bandwidth consumption of AlterWAN packet traffic between said source and destination sites;

a source firewall ~~circuit~~ having a first port for coupling directly or through a local area network to one or more devices at a customer source site, and having an untrusted port coupled to said source router directly or through a local area network, said untrusted port of said source firewall having an Internet Protocol address (hereafter IP address), said source firewall functioning to receive Internet Protocol packets (hereafter IP packets) from said one or more devices at said customer source site which are addressed to one or more devices at a customer destination site (hereafter AlterWAN payload packets) and other IP packets addressed to other locations on the internet (hereafter conventional IP packets), and for encapsulating said AlterWAN payload packets as the payload sections of outgoign AlterWAN ~~IP~~ packets which have as their destination addresses the ~~addressed to an~~ IP address of an untrusted port of a destination firewall at said customer destination site (hereafter outgoing AlterWAN packets) and functioning to encrypt the payloads of said outgoing AlterWAN packets ~~using a first encryption method known to a~~

~~destination firewall and using a key or key known to said destination firewall and which may be user definable~~, and for receiving incoming IP packets and comparing the destination addresses of said incoming IP packets to said IP address of said untrusted port of said source firewall circuit any said incoming IP packet having as its destination address the IP address of said untrusted port of said source firewall being a incoming AlterWAN packet, each said incomimg AlterWAN packet encapsulating as its payload section a AlterWAN payload packet, and decrypting the payload sections of any incoming ~~IP~~ AlterWAN packets ~~having as their destination address the IP address of said untrusted port of said source firewall circuit (hereafter incoming AlterWAN packets) using whatever encryption method and key or keys which were used to encrypt them~~ so as to recover the encapsulated AlterWAN payload packet from each incoming AlterWAN packet, and transmitting each recovered AlterWAN payload packet to a device at said customer source site to which said AlterWAN payload packet is addressed;

one or more routers of ~~other~~ participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers of said ISX/ISP providers functioning to implement said AlterWAN data path as a high bandwidth, low latency, low hop count data path having an average available bandwidth that exceeds the worst case bandwidth consumed by incoming and outgoing AlterWAN packets travelling between said source and destination sites and configured to recognize said incoming and outgoing AlterWAN packets by their destination addresses and route them into said AlterWAN data path. ~~in the form of a virtual private network tunnel through the internet coupling one or more devices at said customer source site to one or more computers at said customer destination site, said low hop count data path having an average available bandwidth which is substantially greater than the worst case bandwidth consumption of AlterWAN packets traveling between said customer source site and said customer destination site;~~

a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated datapath to said router of said endpoint participating ISX/ISP provider and configured to recognize said outgoing AlterWAN packets arriving from said endpoint participating ISX/ISP provider which have travelled from said source firewall via said AlterWAN data path and route them to said destination firewall, and configured to recognize said incoming AlterWAN packets from said destination firewall circuit and route them to said endpoint participating ISX/ISP provider;

~~a~~ said destination firewall circuit having an untrusted port having an IP address to which said outgoing AlterWAN packets are addressed, said untrusted port coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to one or more devices at said customer destination site, said destination firewall circuit configured so as ~~functioning~~ to receive IP packets from said one or more devices at said customer destination site which are addressed to one or more devices at said customer source site (hereafter AlterWAN payload packets) and functioning to receive other conventional IP packets not addresed to any of the said devices at said customer source site, and for encapsulating said AlterWAN payload packets as the payload sections of AlterWAN packets addressed to said IP address of an untrusted port of said source firewall circuit at said customer source site (hereafter incoming ~~outgoing~~ AlterWAN packets) and functioning to encrypt the payloads of said incoming ~~outgoing~~ AlterWAN packets ~~using an encryption method known to said source firewall and a key or keys known to said source firewall~~ and for receiving incoming AlterWAN ~~IP~~ packets and comparing the destination addresses of said incoming AlterWAN ~~IP~~ packets to said IP address of said untrusted port of said destination firewall circuit, and decrypting the payload sections of any incoming AlterWAN ~~IP~~ packets having as their destination address the IP address of said untrusted port of said destination firewall circuit ~~(hereafter incoming AlterWAN packets) using whatever encryption method and key or keys which were used to encrypt said incoming AlterWAN packets~~ so as to recover the encapsulated AlterWAN payload packet from each incoming AlterWAN packet, and transmitting each recovered AlterWAN payload packet to the device to which it is addressed at said customer destination site.

Please add the following new claims:

11. (new) A method of doing business to establish a private bidirectional wide area network between a source site and a destination site using the internet as a backbone, comprising the steps:

connecting one or more computing devices at a source site to a firewall and source router and obtaining a known IP address for each computing device at said source site;

connecting one or more computing devices at a destination site to a firewall and destination router and obtaining a known IP address for each computing device at said destination site;

selecting one or more participating ISX/ISP internet service providers which have one or more high bandwidth, low latency, low hop count data paths that can be used as at least part of a high bandwidth, low latency, low hop count data path for transmission of AlterWAN data packets between said source site and said destination site (hereafter referred to as the AlterWAN data path), and making agreements with said participating ISX/ISP internet service providers to always route AlterWAN packets into said AlterWAN data path such that said AlterWAN data packets will only travel on AlterWAN data path, wherein said AlterWAN packets are defined as packets which contain as a destination address one of said known IP addresses of computing devices at said source site or said destination site, and ensuring that said routing tables of routers of said one or more participating ISX/ISP internet service providers either already contain routing statements that will cause AlterWAN packets to be routed into said AlterWAN data path or are modified to contain such route statements;

connecting said source router and said destination router to one of said participating ISX/ISP internet service providers through dedicated high bandwidth, low latency data paths.

12. [new] A method comprising:

generating an Internet Protocol data packet (hereafter IP packet) having as its destination address an Internet Protocol address assigned to a computing device at the other end of a private, wide area network using the internet as a backbone (hereafter referred to as an AlterWAN private tunnel);

encrypting a payload portion of said IP packet to generate an encrypted IP packet;

generating a composite AlterWAN packet by encapsulating said encrypted IP packet in another IP packet having as its destination address an IP address of an untrusted side of a firewall which is at a destination site which is part of said AlterWAN private tunnel; and

routing said composite AlterWAN packet using a source router whose routing table has been configured to include a routing statement which recognizes said destination address of said composite AlterWAN packet and routes said composite AlterWAN packet via a dedicated data path to an AlterWAN data path, said AlterWAN data path being defined as a high bandwidth, low latency, low hop count data path provided by one or more participating ISX/ISP internet service providers that links said source site and said destination site of said AlterWAN private tunnel, each participating ISX/ISP internet service provider being one which has been selected as having at least one high bandwidth, low latency, low hop count data path which can be used to transmit said composite AlterWAN data packet either from said source site to said destination site or to another participating ISX/ISP internet service provider and which has routers which either already contain or which are configured to contain predetermined routing statements when said participating ISX/ISP agrees to provide routing services as part of said AlterWAN data path, said predetermined routing statements being ones which will recognize said IP destination address of each said composite AlterWAN data packets and cause said composite AlterWAN packets to be routed into said AlterWAN data path.

13. [new] A method comprising:

receiving composite AlterWAN packet comprised of an encapsulating IP packet having as its destination address an Internet Protocol address assigned to a firewall at said destination site and using said Internet Protocol address assigned to said firewall in the destination address field of said encapsulating IP packet to recognize said packet as a composite AlterWAN packet, said encapsulating IP packet including at its payload an encrypted IP packet having as its destination address an Internet Protocol address of a computing device at said destination site, said destination site being at an end of a private, wide area network using the internet as a backbone (hereafter referred to as an AlterWAN private tunnel) and reacting to recognition of said received packet as an AlterWAN composite packet by routing said composite AlterWAN packet to a firewall;

in said firewall, decrypting a payload portion of said encrypted IP packet to generate a recovered IP packet;

routing said recovered IP packet to a computing device to which said recovered IP packet is addressed.

14. [new] A method of doing business comprising:

selecting one or more participating ISX/ISP internet service providers which have one or more high bandwidth, low latency, low hop count data paths that can be used as at least part of a high bandwidth, low latency, low hop count data path for transmission of composite AlterWAN data packets between a source site and a destination site of a private wide area network using the internet as a backbone (hereafter referred to as the AlterWAN data path), where composite AlterWAN data packets are defined as internet protocol packets (hereafter the outer packet) which encapsulate other internet protocol packets (hereafter the inner packet), said inner packet having as its destination address the IP address of a computing device at one end of said AlterWAN data path and at least the payload section of said inner packet being encrypted, said outer packet having as its destination address an IP address of an untrusted side of a firewall at the same end of said AlterWAN data path as said computing device which has as its IP address said destination address of said inner packet;

making agreements with said participating ISX/ISP internet service providers to always route composite AlterWAN packets into said AlterWAN data path such that said composite AlterWAN data packets will only travel on said AlterWAN data path;

ensuring that said routing tables of routers of said one or more participating ISX/ISP internet service providers either already contain routing statements that will cause said composite AlterWAN data packets to be recognized and routed into said AlterWAN data path or are modified to contain such route statements.

15. [new] A method of doing business comprising:

selecting one or more participating ISX/ISP internet service providers which have one or more high bandwidth, low latency, low hop count data paths that can be used as at least part of a high bandwidth, low latency, low hop count data path for transmission of AlterWAN data packets between a source site and a destination site of a wide area network using the internet as a backbone (hereafter referred to as the AlterWAN data path), where AlterWAN data packets are defined as internet protocol packets which contain as a destination address one of said known IP addresses of computing devices at said source site or said destination site;

making agreements with said participating ISX/ISP internet service providers to always route said AlterWAN packets into said AlterWAN data path such that said AlterWAN data packets will only travel on said AlterWAN data path;

ensuring that said routing tables of routers of said one or more participating ISX/ISP internet service providers either already contain routing statements that will cause said AlterWAN data packets to be recognized and routed into said AlterWAN data path or are modified to contain such route statements.

16. [new] A method of operating a router at an ISX/ISP comprising the steps:

using said router to recognize AlterWAN data packets where AlterWAN data packets are defined as internet protocol packets which contain as a destination address one of one or more known IP addresses of computing devices at a source site or a destination site of a wide area network using the internet as a backbone;

looking up routing statements that are applicable to said AlterWAN data packets and using said routing statements to route said AlterWAN data packets into a high bandwidth, low latency, low hop count data path coupling said soure site to said destination site.

17. [new] A method of operating a router at an ISX/ISP comprising the steps:

using said router to recognize composite AlterWAN data packets where composite AlterWAN data packets are defined as internet protocol packets (hereafter the outer packet) which encapsulate other internet protocol packets (hereafter the inner packet), said inner packet having as its destination address one of one or more known IP addresses of computing devices at a source site or a destination site of a wide area network using the internet as a backbone and at least the payload section of said inner packet being encrypted, said outer packet having as its destination address an IP address of an untrusted side of a firewall at the same end of said AlterWAN data path as said computing device which has as its IP address said destination address of said inner packet;

looking up routing statements that are applicable to said composite AlterWAN data packets and using said routing statements to route said composite AlterWAN data packets into a high bandwidth, low latency, low hop count data path coupling said soure site to said destination site.

18. [new] A router at an ISX/ISP which is part of a private wide area network using the internet as a backbone, said router being conventional except that said router is coupled to a high bandwidth, low latency, low hop count data path and has been configured to contain routing statements that cause AlterWAN data packets to be recognized and routed into said high bandwidth, low latency, low hop count data path, where AlterWAN data packets are defined as internet protocol packets which contain as a destination address one of one or more known IP addresses of computing devices at a source site or a destination site of a wide area network using the internet as a backbone.

19. [new] A router at an ISX/ISP which is part of a private wide area network using the internet as a backbone, said router being conventional except that said router is coupled to a

high bandwidth, low latency, low hop count data path and has been configured to contain routing statements that cause composite AlterWAN data packets to be recognized and routed into said high bandwidth, low latency, low hop count data path, where composite AlterWAN data packets are defined as internet protocol packets (hereafter the outer packet) which encapsulate other internet protocol packets (hereafter the inner packet), said inner packet having as its destination address one of one or more known IP addresses of computing devices at a source site or a destination site of a wide area network using the internet as a backbone and at least the payload section of said inner packet being encrypted, said outer packet having as its destination address an IP address of an untrusted side of a firewall at the same end of said AlterWAN data path as said computing device which has as its IP address said destination address of said inner packet.